Marked-up version of the amended claims--additions are shown with double-underlines and deletions are shown with strike-throughs.

1. A method of enabling a client terminal user to access target resources managed by a set of resource managers within an enterprise computing environment, comprising:

authenticating the user to establish a user primary identity;

mapping the user primary identity to a set of user secondary identities;

authenticating the user to the resource managers using the set of user secondary identities;

following authentication using the set of user secondary identities, forwarding resource requests to the resource managers; and

returning replies received from the resource managers back to the user.

2. The method as described in claim 1 wherein the user primary identity is mapped to the set of user secondary identities by a sign-on service.

3. The method as described in claim 2 further including the step of authenticating a trusted server to the sign-on service prior to mapping the user primary identity to the set of user secondary identities.

4. The method as described in claim 3 wherein the trusted server is authenticated to the sign-on server before the step of authenticating the user to establish the user primary identity.

5. The method as described in claim 3 wherein the trusted server is authenticated to the sign-on service after the step of authenticating the user to establish the user primary identity.

6. The method as described in claim 3 wherein the user is authenticated to establish the user primary identity using an authentication service associated with the trusted server.

7. The method as described in claim 1 further including the step of load balancing resource requests across a set of instances of a given resource manager.

8. The method as described in claim 1 wherein the client terminal user accesses the enterprise computing environment over the Internet.

9. The method as described in claim 1 wherein the user is authenticated to a given resource manager using an authentication service associated with the given resource manager.

10. (Amended) A method for enabling a client terminal user to access target resources managed by a set of resource managers operative within an enterprise computing environment, wherein the environment has an associated sign-on service, comprising:

responsive to a request received from a user of the client terminal, authenticating the user to establish a~~n~~ user primary identity;

using the user primary identity, accessing the sign-on service to retrieve a set of stored user authentication information, wherein the stored user authentication information comprises a set of user secondary identities;

performing a sign-on to the set of resource managers using the retrieved set of user secondary identities; and ~~user authentication information; and~~

forwarding the request to a given resource manager; and

forwarding a reply received from the given resource manager back to the user.

11. A method for enabling a client terminal user to access target resources managed by a set of resource managers operative within an enterprise computing environment, wherein the environment has an associated sign-on service, comprising:

having the client terminal user perform a primary logon to an intermediary server to establish a user primary identity;

having the intermediary server pass the user's primary identity to the sign-on service and, in response, obtaining a set of user secondary identities that may be used in enabling the intermediary server to represent the client terminal user to the resource managers;

having the intermediary server perform a secondary logon to a first resource manager using a first user secondary identity;

having the intermediary server perform a secondary logon to a second resource manager using a second user secondary identity;

having the intermediary server perform resource requests at the first and second resource managers under the respective secondary identities; and

forwarding responses back to the client terminal user.

12. (Amended) ~~In an~~ An enterprise computing environment having a set of resource managers and a sign-on service, the ~~improvement~~ enterprise computing environment comprising:

~~a server (a)~~

means for authenticating a user to establish a user primary account associated with a user primary identity;~~, (b)~~

means for cooperating with the sign-on service to map ~~delegate~~ the user primary account to a set of user secondary accounts associated with a set of user secondary identities; ~~(c)~~

means for logging onto the set of resource managers using the user secondary accounts; and ~~(d)~~

means for passing resource requests from the user to the resource managers under the user secondary accounts.

13. (Amended) ~~In the~~ The enterprise computing environment as described in claim 12 wherein the server passes replies to the resource requests back to the user.

14. (Amended) A server for use in an enterprise computing environment having a set of resource managers and a sign-on service, comprising:

means for authenticating a user to establish a user primary account, associated with a user primary identity;

means for authenticating the server to the sign-on service;

means for logging onto the set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts is associated with a set of user secondary identities; and

means for passing resource requests and associated replies between the user and the resource managers.

15. The server as described in claim 14 further including means for load balancing resource requests passed to a set of instances of a given resource manager.

16. (Amended) A system, comprising:

a set of resource managers;

a sign on service;

a server, comprising:

means for authenticating users to establish user primary accounts, associated with primary user identities;

means for logging a given user onto the set of resource managers using a set of user secondary accounts for the given user retrieved from the sign on service, wherein a set of user secondary accounts for a given user is associated with a set of user secondary identities for a given user; and

means for passing resource requests and associated replies between the given user and the resource managers.

17. The system as described in claim 16 wherein at least one resource manager comprises a set of instances.

18. The system as described in claim 17 wherein the server further includes means for load balancing resource requests across the set of instances.

19. The system as described in claim 16 wherein the server comprises a set of instances.

20. The system as described in claim 19 further including a manager that manages the set of server instances.

21. (Amended) A computer program product in a computer-useable medium executable in a processor of a server, comprising:

means for authenticating a user to establish a user primary account associated with a user primary identity;

means for authenticating the server to a sign-on service;

means for logging onto a set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts are associated with a set of user secondary identities; and

means for passing resource requests and associated replies between the user and the resource managers.

II. General Remarks Concerning This Response

Claims 1-21 are currently pending in the present application. Claims 10, 12-14, 16, and 21 have been amended in this response; no claims have been added or canceled. Reconsideration of the claims is requested.

III. Summary of Present Invention

An enterprise computing environment, such as a corporate web portal, includes an intermediary server, a sign-on service, and one or more backend enterprise systems managed by resource managers. Before or after user primary logon, which establishes a user primary account identity, the intermediary server uses its own identity to authenticate to the sign-on service its right to retrieve user secondary account identities with respect to the backend enterprise systems. Retrieved secondary account identities are then used by the intermediary server to perform user secondary logons to respective resource managers in the environment. The intermediary server also manages the passing of resource requests and associated replies between the user and the resource managers.

IV. 35 U.S.C. § 102(e)-Anticipation—*Grantges*

The Office action has rejected independent claims 1-6, 8-14, 16, 17, and 19-21 under 35 U.S.C. § 102(e) as anticipated by Grantges, "Secure Gateway Having User Identification and Password Authentication", U.S. Patent No. 6,324,648, filed 12/14/1999, issued 11/27/2001. This rejection is respectfully traversed.

All of the pending independent claims have been rejected over Grantges. Each of these independent claims has one or more common elements, and the rejection applies certain portions of Grantges against these common elements. However, Applicant asserts that there is at least element of each independent claim that is not shown in Grantges; some of these elements were in the original claims while others have been added to the amended claims in this response. Prior to addressing each of the independent claims, Applicant makes the following remarks regarding the manner in which the rejection has applied certain sections of Grantges to the elements that are shared in common by the independent claims.

Grantges discloses a distributed data processing system which has a proxy server in a DMZ on the exterior of a firewall that is protecting the distributed data processing system. On the interior of the firewall, an application gateway supports another proxy server. Each of the proxy servers employs some form of security to restrict access to the system. When the proxy server in the DMZ receives a request, e.g., from a user browser, it attempts to authenticate the user that has made the request. If the user is authenticated, then the proxy server in the DMZ forwards the request to the proxy server inside the firewall; the proxy server in the DMZ does not interact directly with the application servers inside the firewall. When the proxy server inside the firewall receives the request, it may forward the request to an application server, or it may perform some additional authorization security procedures. In this manner, only the proxy servers communicate through the firewall.

However, in the system disclosed in Grantges, there is only one user identity that is associated with the user that is making a request. Grantges does not disclose a plurality of user identities, such as a primary user identity and a set of secondary user identities as disclosed and claimed in the present patent application. For example, when a digital certificate is associated with a user request, the proxy server in the DMZ may perform an authentication process with the certificate, which is then forwarded along with the request to the proxy server inside the firewall, at which point the second proxy server may also use the certificate. As is well-known, though, a digital certificate binds a single user identity with a particular user.

Applicant asserts that the rejection has misinterpreted the manner in which the system of Grantges employs a single user identity and improperly states that Grantges discloses the employment of multiple user identities. For example, the Office action states that the feature of "authenticating the user to the resource managers using the set of user secondary identities" in claim 1 is disclosed at column 4, lines 49-52, which reads: "If authenticated at this level, proxy server 34 then sends the information contained in the client's digital certificate through firewall system 32 to gateway 38 to be authenticated at a second, more substantive level." However, Grantges continues: "The second level authentication involves examining the particulars of the X.509 digital certificate using the data stored on authorization server 46." In other words, the system of Grantges continues processing with the single identity that has been verified by the certificate. As is well known, a digital certificate is used to verify a single entity's identity, and in Grantges, a single identity associated with a digital certificate is authenticated. While the system of Grantges may perform additional processing using information from various databases, Grantges does not disclose multiple user identities for a given user.

Moreover, the rejection has apparently equated the proxy server inside the gateway as a type of single sign-on service because it is responsible for performing any security operations that might be required to be performed inside the firewall prior to forwarding a request to an application server. Continuing with the issue of a plurality of user identities for a given user, the Office action states that the feature of "mapping the user primary identity to a set of user secondary identities" in claim 1 is disclosed at column 5, lines 65-67, and column 8, lines 53-59 and lines 62-65. These sections read substantially as follows.

> "Proxy servers in general may be characterized as providing both mapping and data caching functions. In the context of the present invention, DMZ proxy server 34 is provided principally for mapping purposes."

> "A second level authentication is commenced with a message 72. This authentication is done by comparing data from the digital certificate provided by client computer 22 with predetermined data about the certificate on authorization server 46. To secure the transfer of the digital certificate across firewall 32, DMZ proxy server 34 and gateway proxy server 40 establish second secure connection 54, shown in FIG. 1. It bears emphasizing that DMZ proxy server 34 only knows the URL of application gateway proxy server 40, which is kept in a local configuration file (behind the firewall), provides the URL/addresses of the destination servers."

The mapping that is discussed in Grantges is more of a routing function, as disclosed at column 7, lines 1-5:

> Gateway proxy server 40 further performs well-known mapping functions, and, in accordance with the present invention, efficiently routes messages destined for various applications 24_1, 24_2, ... 24_3 to the appropriate one of the destination servers 28_1, 28_2, ... 28_3.

This mapping in the system of Grantges is not disclosed as the claimed mapping of a primary user identity to a set of secondary user identities.

With reference now to independent claim 1, Applicant asserts that Grantges does not disclose the elements of "mapping the user primary identity ..." and "authenticating the user to the resource managers using the set of user secondary identities" because, as explained above, Grantges does not disclose the use of multiple user identities associated with a single user. Hence, Grantges does not disclose at least one element of claim 1 as is required for a proper anticipation rejection. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, the rejection of claim 1 is improper, and Applicant requests that the rejection be withdrawn.

Dependent claims 2-9 are patentable for the same reasons as independent claim 1 based on their incorporation of claim 1. Dependent claim 7 is addressed by an obviousness-type rejection. Dependent claim 8 merely states that the client uses the Internet, while dependent claim 9 merely states that an authentication service that is associated with a resource manager performs an authentication operation. However, dependent claims 2-6 incorporate some form of processing on a set of secondary user identities, so these features also are not disclosed in Grantges, thereby providing additional reasons for the patentability of claims 2-6.

Independent claim 10 has been amended to distinguish it from Grantges. For example, amended claim 10 now includes the elements of "using the user primary identity, accessing the sign-on service to retrieve a set of stored user authentication information, wherein the stored user authentication information comprises a set of user secondary identities" and "performing a sign-on to the set of resource managers using the retrieved set of user secondary identities". Hence, for reasons similar to those that were argued above with respect to independent claim 1, amended independent claim 10 now includes features that are not disclosed in Grantges, and claim 10 is also patentable because Grantges does not disclose at least one element of claim 10 as is required for a proper anticipation rejection.

With respect to independent claim 11, this claim also recites various elements concerning a user primary identity and a set of user secondary identities. Hence, for reasons similar to those that were argued above with respect to independent claim 1, independent claim 11 has features that are not disclosed in Grantges, and claim 11 is also patentable because Grantges does not disclose at least one element of claim 11 as is required for a proper anticipation rejection.

Independent claim 12 has been amended to distinguish it from Grantges. For example, amended claim 12 now includes the elements of "means for authenticating a user to establish a user primary account associated with a user primary identity" and "means for cooperating with the sign-on service to map the user primary account to a set of user secondary accounts associated with a set of user secondary identities". Hence, for reasons similar to those that were argued above with respect to independent claim 1, amended independent claim 12 now includes features that are not disclosed in Grantges, and claim 12 is also patentable because Grantges does not disclose at least one element of claim 10 as is required for a proper anticipation rejection.

Dependent claim 13 merely states that the server returns replies to the user, but dependent claim 13 is patentable for the same reasons as independent claim 12 based on its incorporation of claim 12.

Independent claim 14 has been amended to distinguish it from Grantges. For example, amended claim 14 now includes the elements of "means for authenticating a user to establish a user primary account associated with a user primary identity" and "means for logging onto the set of resource managers using a set of user secondary accounts returned from the sign-on service, wherein the set of user secondary accounts is associated with a set of user secondary identities". Hence, for reasons similar to those that were argued above with respect to independent claim 1, amended independent claim 14 now includes features that are not disclosed in Grantges, and claim 14 is also patentable because Grantges does not disclose at least one element of claim 14 as is required for a proper anticipation rejection. Dependent claim 15, which depends from claim 14, is addressed in a obviousness-type rejection.

Independent claim 16 has been amended to distinguish it from Grantges. For example, amended claim 16 now includes the elements of "means for authenticating users to establish user primary accounts associated with user primary identities" and "means for logging a given user onto the set of resource managers using a set of user secondary accounts for the given user retrieved from the sign on service, wherein a set of user secondary accounts for a given user is associated with a set of user secondary identities for a given user". Hence, for reasons similar to those that were argued above with respect to independent claim 1, amended independent claim 16 now includes features that are not disclosed in Grantges, and claim 16 is also patentable because Grantges does not disclose at least one element of claim 16 as is required for a proper anticipation rejection.

Dependent claims 17-20 are patentable for the same reasons as independent claim 16 based on their incorporation of claim 16. Dependent claim 18, which depends from claim 16, is addressed in a obviousness-type rejection. Dependent claims 17, 19, and 20 merely recite a plurality of servers or resource managers.

Independent claim 21 has been amended to distinguish it from Grantges. Claim 21 is similar to claim 14; claim 21 is directed to a computer program product, whereas claim 14 is directed to a server. Hence, for reasons similar to those that were argued above with respect to independent claims 1 and 14, amended independent claim 21 now includes features that are not disclosed in Grantges, and claim 21 is also patentable because Grantges does not disclose at least one element of claim 21 as is required for a proper anticipation rejection.

V. 35 U.S.C. § 103(a)-Obviousness-*Grantges* in view of *Brendel et al.*

The Office action has rejected claims 7, 15, and 18 under 35 U.S.C. § 103(a) as unpatentable over Grantges et al. in view of Brendel et al., "World-Wide-Web Server with Delayed Resource-Binding for Resource-Based Load Balancing on A Distributed Resource Multi-Node Network, filed 08/05/1996, issued 06/30/1998. This rejection is respectfully traversed.

With respect to dependent claims 7, 15, and 18, the rejection properly states that Brendel et al. discloses a load-balancing mechanism as recited in claims 7, 15, and 18. However, claims 7, 15, and 18 depend from claims 1, 14, and 16, respectively, and as argued above, Grantges fails to disclose the features of these independent claims. Hence, a combination of the teaching of <u>Bereiter</u> with <u>Grantges</u> cannot support a rejection of dependent claims 7, 15, and 18 because at least one feature of the independent claims has not been disclosed in the prior art. Applicant respectfully submits that more than one claimed feature is not shown in the prior art references nor can the teachings of the references be combined to disclose the present invention. Hence, the rejection of claims 7, 15, and 18 does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of claims 7, 15, and 18 under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied references. Applicant requests that the rejection be withdrawn.

VI. <u>Conclusion</u>

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: <u>March 21, 2003</u>

Respectfully submitted,

Joseph R Burwell

Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz